1. Mô hình OSI

+Là một thiết kế dựa vào nguyên lý tầng cấp. lý giải 1 cách trừu tượng kỹ thuật kết nối truyền thông giữa các máy vi tính và thiết kế giao thức mạng giữa chúng

+Chỉ được ngành công nghiệp mạng và công nghệ thông tin tôn trọng 1 cách tương đối, tính năng chính của nó là quy định về giao diện giữa các tầng cấp, tức quy định đặc tả về các phương pháp và các tầng liên lạc với nhau

+có 7 tầng:

. tầng vật lý

. tầng liên kết dữ liệu: Đây chính là nơi các thiết bị chuyển mạch (switches) hoạt động. Kết nối chỉ được cung cấp giữa các nút mạng được nối với nhau trong nội bộ mạng

. tầng mạng

. tầng giao vận

. tầng phiên

. tầng trình diễn

. tầng ứng dụng

2. TCP

(Transmission Control Protocol) Là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các kết nối với nhau, mà qua đó chúng có thể trao đổi dữ liệu hoặc các gói tin

3. LAN

LAN (mạng máy tính cục bộ) là mạng máy tính nội bộ, kết nối các máy tính trong một phạm vi nhỏ. Những máy kết nối mạng LAN hiện đại có thể giao tiếp với nhau cũng như với các máy tính ngoài. Nhưng những máy tính khác không thể bắt đầu liên lạc ngược lại. Đó bởi vì mạng cục bộ của bạn được thiết kế “riêng tư” với tiêu chuẩn IPv4.

4. Router

router chính là một thiết bị để chia sẻ Internet tới nhiều các thiết bị khác trong cùng lớp mạng. Một router điển hình hiện nay là bộ định tuyến không dây có phát sóng Wi-Fi (một số nơi gọi là access point hay AP). Hiện nay, các bộ định tuyến không dây thường được trang bị một hoặc nhiều ăng-ten, vài người quen gọi là "râu" cho phép họ có thể điều chỉnh được để cải thiện hướng sóng.

Thiết bị này cho phép tạo ra một mạng Wi-Fi sử dụng cho rất nhiều các thiết bị khác. Bên cạnh đó, các router thường có khá nhiều cổng Ethernet (còn gọi là cổng LAN) cho phép người dùng có thể kết nối được nhiều với các thiết bị khác thông qua cáp nối (mạng có dây hoặc hữu tuyến).

Router nhận dữ liệu Internet từ một modem và mỗi router sẽ có một địa chỉ IP công khai duy nhất trên Internet. Các máy chủ trên mạng Internet sẽ kết nối với router thông qua modem và thiết bị này có nhiệm vụ định tuyến lưu lượng truy cập đến các thiết bị khác trong mạng.

Tuy nhiên chỉ với một router (không phải loại 2-trong-1), sẽ khó có thể kết nối được với Internet. Bộ định tuyến sẽ chỉ có thể kết nối với Internet bằng cách nối cáp Ethernet chuyên biệt với một chiếc modem.

5. Modem

Nếu ví router là đứa con thì modem chính là người mẹ. Nếu không có modem, router chỉ thực hiện được chức năng thiết lập mạng nội bộ chứ không thể kết nối ra Internet quốc tế.

Modem là thiết bị giao tiếp với mạng lưới của các nhà cung cấp dịch vụ Internet (ISP).

Thông qua hệ thống cáp nối đồng trục hoặc cáp quang từ các trạm cung cấp Internet nối đến nhà bạn, modem sẽ đóng vai trò chuyển hóa các gói dữ liệu do ISP cung cấp thành kết nối Internet cho router hoặc các thiết bị có liên kết mạng khác. Trong khi đó, modem DSL (dạng quay số) kết nối trực tiếp tới đường dây điện thoại.

5. Repeater

Trong hệ thống mạng LAN, khoảng cách truyền dẫn tín hiệu tối đa là 100m, đối với dây cáp mạng UTP CAT5e. Do đó, khi khách hàng muốn truyền tín hiệu ở một khoảng cách xa hơn thì cần một bộ khuếch đại và định thời lại tín hiệu, giúp tín hiệu có thể truyền dẫn đi xa hơn giới hạn 100m này. REPEATER chính là một thiết bị như trên

6. Hub

Hub có thể được xem là một Repeater có nhiều cổng. Một Hub có từ 4 đến 24 cổng và có thể còn nhiều hơn. Trong phần lớn các trường hợp, Hub được sử dụng trong các mạng 10BASE-T hay 100BASE-T. Khi cấu hình mạng là hình sao (Star topology), Hub đóng vai trò là trung tâm của mạng. Với một Hub, khi thông tin vào từ một cổng và sẽ được đưa đến tất cả các cổng khác.

Hub có 2 loại là Active Hub và Smart Hub. Active Hub là loại Hub được dùng phổ biến, cần được cấp nguồn khi hoạt động, được sử dụng để khuếch đại tín hiệu đến và cho tín hiệu ra những cổng còn lại, đảm bảo mức tín hiệu cần thiết. Smart Hub (Intelligent Hub) có chức năng tương tự như Active Hub, nhưng có tích hợp thêm chip có khả năng tự động dò lỗi – rất hữu ích trong trường hợp dò tìm và phát hiện lỗi trong mạng.

7. Bridge

Bridge là gì? Bridge là một thiết bị được dùng để ghép nối 2 mạng khác nhau để tạo thành một mạng lớn duy nhất. Bridge quan sát các gói tin (packet) trên mọi mạng khác nhau. Nếu có một gói tin được gởi từ mạng này sang một mạng khách. Bridge sẽ sao chép lại gói tin này, đồng thời gởi nó đến mạng đích.

8. Switch

Switch là gì? Switch có thể được xem là một Bridge có nhiều cổng. Switch có thể liên kết được nhiều Segment lại với nhau. Số lượng Segment tuỳ thuộc vào số cổng (Port) trên Switch. Tương tự như cách hoạt động của Bridge, Switch cũng sao chép các gói tin mà nó nhận được từ các máy trong mạng, sau đó, Switch tổng hợp các gói tin này lên bảng Switch, bảng này có vai trò cung cấp thông tin nhằm giúp các gói tin được gởi đến đúng địa chỉ trong hệ thống mạng.

Ngoài ra, Switch còn có một khả năng khách là tạo mạng LAN ảo (VLAN) nhằm tăng hiệu quả của việc sử dụng hệ thống mạng LAN thông qua việc tăng tính bảo mật, kha thác tối đa lợi ích sử dụng của các cổng ( Port) hay tăng cường tính linh động trong việc thêm hoặc bớt máy vào hệ thống mạng.

9. Gateway

Gateway có thể chuyển đổi giao thức của một mạng thành một giao thức khác, thông qua đó, kết nối các mạng có giao thức khác nhau lại với nhau.

5. Ethernet

Ethernet là một trong số những phương tiện mà bạn có thể sử dụng để tạo ra một mạng LAN, bao gồm cả Wi-Fi, Bluetooth và USB. Những thứ này có thể được sử dụng để tạo ra một mạng cục bộ hoặc có thể cùng tồn tại trong cùng một mạng. Trong khi mạng không dây có sự tiện lợi riêng của nó thì Ethernet vẫn giữ nhiều vai trò quan trọng, như:

* Ethernet vẫn là kết nối facto cho những máy trạm trong các mạng doanh nghiệp.
* Kể cả khi trong mạng không dây hoàn chỉnh (mạng gia đình) thì kết nối giữa cáp / DSL modem và router là Ethernet.
* Các hoạt động băng thông như chơi trò chơi hay phát trực tuyến vẫn được hưởng lợi từ kết nối Ethernet có dây.
* Mạng Ethernet tiếp tục cung cấp lợi ích của bảo mật vật lý

Những phần chính của thiết bị mạng trong một mạng Ethernet là cáp Category-5 mà chạy giữa hai cổng RJ-45. Một mạng Ethernet cơ bản có thể chứa ba phần: hai nút với cổng RS-45 và cáp chạy giữa chúng. Trong một mạng gia đình, điều này tương đương với việc cắm thiết bị của bạn (như Xbox) trực tiếp vào cổng của modem cáp.

Các mạng phức tạp hơn sử dụng các yếu tố như hub và router. Điều quan trọng để nhớ là các hub kết nối mạng nội bộ và router kết nối nó với những mạng bên ngoài. Tất cả đều có thể kết hợp với một mạng bao gồm các kết nối Ethernet tới những thiết bị như máy tính hoặc máy chủ và các kết nối không dây với máy in, điện thoại, máy tính bảng, thiết bị ngoài phạm vi có dây.

10. Multilayer switch (MLS)

Là một thuật ngữ để chỉ công nghệ sử dụng phần cứng để forwarding dựa trên thông tin của nhiều layer trên mô hình OSI.

Theo Cisco, hoạt động của các Multilayer Switch gồm 2 loại:

* Route caching: Đây là thế hệ đầu tiên, còn được gọi là MLS, Netflow LAN switching, flow-based hay demand-based switching
* Topology-based: Đây là thế hệ thứ hai, còn được biết đến với cái tên Cisco Express Forwarding (CEF)

Đối với MLS, thiết bị được yêu cầu có hai thành phần là Route Processor (RP) và Switch Engine (SE). Ngoài ra, hai thành phần này dùng Multilayer Switching Protocol (MLSP) để triển khai hoạt động.

Hoạt động của MLS dựa vào các bảng:

1. CAM (Content-Addressable Memory) hay còn gọi là bảng MAC, đây là một thành phần cơ bản của switch. Bảng cấu trúc thành từng dòng, các thông tin trong 1 dòng gồm: port, địa chỉ MAC tương ứng, VLAN tương ứng.
2. TCAM (Ternary Content-Addressable Memory) cũng là một thành phần cơ bản quan trọng của switch. Từ “ternary” mang nghĩa là 3 trạng thái: 0, 1 và X. Đây là nơi các access control list (ACLs) đặt vào, có thể là security ACLs hoặc QoS ACLs. Một switch có thể chứa nhiều TCAM.

Đối với MLS, TCAM còn dùng để định nghĩa các flow – gọi là flow mask, cụ thể như sau:

* Nếu không có ACL, một flow là các packet cùng IP đích.
* Nếu có standard ACLs, một flow là các packet cùng địa chỉ IP nguồn và đích.
* Nếu có extended ACLs, một flow là các packet cùng địa chỉ IP nguồn, IP đích, protocol và port.

MLS cache là bảng chứa các entry về flow, kích thước tối đa 128K. Entry lưu trong cache có “aging time” để loại bỏ những flow không dùng đến nữa.

**Cơ chế**

Cơ chế của MLS là “route once, switch many”.

Đối với một flow, RP sẽ thực hiện chức năng routing của mình đối với packet đầu tiên – trong khi đó MLSP giúp SE học các entry về flow đó vào cache. Các packet sau đó SE sẽ thực hiện switching mà không cần RP nữa.

Một packet khi đến sẽ được kiểm tra thông tin header với các entry lưu trong cache. Nếu có thì thực hiện quá trình switching. Nếu không thì đây được coi là một flow mới và RP sẽ nhận nhiệm vụ xử lý.

**Ưu và nhược điểm của MLS**

MLS nhanh hơn router về mặt forwarding nhờ sử dụng phần cứng.

Hoạt động của MLS chỉ gặp vấn đề thực sự khi hệ thống mạng bất ổn và thay đổi nhiều lần trong thời gian ngắn (do các neighbor, route,…). Khi đó MLS cache sẽ liên tục phải xây dựng lại và RP hoạt động nhiều gây hao tổn tài nguyên và giảm hiệu suất.

“Aging time” có thể là vấn đề làm phình to kích thước dữ liệu trong một cache giới hạn, đó là khi lưu lượng mạng lớn, trong đó có nhiều packet chỉ xuất hiện trong thời gian ngắn.

12. Unicast

Unicast là 1 thuật ngữ được sử dụng để mô tả cách thức truyền tin được gửi từ 1 điểm đến 1 điểm khác. Trong trường hợp này chỉ có 1 nguồn gửi và 1 nguồn nhận.

Việc truyền Unicast, trong đó 1 gói tin được gửi từ 1 nguồn duy nhất đến 1 địa điểm được quy định, vẫn là hình thức truyền chủ yếu trong mạng LAN và Internet.Tất cả các mạng LAN (VD: Ethernet) và mạng IP hỗ trợ chế độ Unicast, các ứng dụng sử dụng phương thức vận chuyển giao thức TCP ví dụ như Http, Smtp, Ftp, Telnet).

13. Broadcast

Broadcast là thuật ngữ được sử dụng để mô tả cách thức truyền tin được gửi từ 1 điểm đến tất cả các điểm khác. Trong trường hợp này, có 1 nguồn gửi nhưng thông tin được gửi đến tất cả các nguồn nhận trong cùng 1 kết nối.

Broadcast được hỗ trợ trong hầu hết các mạng LAN (VD: Ethernet), được sử dụng để gửi cùng 1 thông điệp cho tất cả các máy tính trong mạng LAN (ví dụ như bản tin ARP: giao thức phân giải địa chỉ, truy vấn địa chỉ của tất cả các máy tính trong cùng 1 mạng LAN). Giao thức lớp mạng (Ipv4) cũng hỗ trợ kiểu truyền Broadcast, cho phép các gói tin được gửi đến mọi thiết bị trong cùng 1 mạng

14. Multicast

Multicast là thuật ngữ được sử dụng để mô tả cách thức truyền tin được gửi từ 1 hoặc nhiều điểm đến 1 tập hợp các điểm khác. Trong trường hợp này có thể là 1 hoặc nhiều người gửi, và thông tin được phân phối cho 1 tập hợp các điểm thu.Multicast hữu ích nếu 1 nhóm khách hàng yêu cầu 1 bộ dữ liệu chung cùng 1 lúc. Việc truyền Multicast sẽ có thể tiết kiệm băng thông 1 cách đáng kể

15. VLAN

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, ứng dụng… của công ty. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai trò tạo ra miền quảng bá. Đối với VLAN, switch có thể tạo ra miền quảng bá.

Việc này được thực hiện khi bạn - quản trị viên - đặt một số cổng switch trong VLAN ngoại trừ VLAN 1 - VLAN mặc định. Tất cả các cổng trong một mạng VLAN đơn đều thuộc một miền quảng bá duy nhất.

Vì các switch có thể giao tiếp với nhau nên một số cổng trên switch A có thể nằm trong VLAN 10 và một số cổng trên switch B cũng có thể trong VLAN 10. Các bản tin quảng bá giữa những máy tính này sẽ không bị lộ trên các cổng thuộc bất kỳ VLAN nào ngoại trừ VLAN 10. Tuy nhiên, tất cả các máy tính này đều có thể giao tiếp với nhau vì chúng thuộc cùng một VLAN. Nếu không được cấu hình bổ sung, chúng sẽ không thể giao tiếp với các máy tính khác nằm ngoài VLAN này.

16. VXLAN

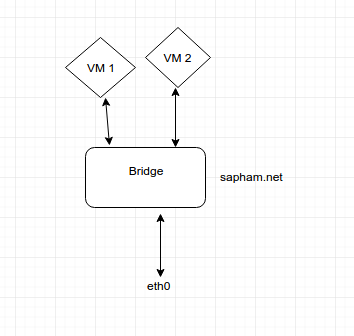
* **VXLAN (Virtual eXtensible LANs)**: đây là công nghệ cung cấp dịch vụ để kết nối Ethernet tới các thiết bị cuối như VLAN ngày nay, nhưng có nhiều tính năng mở rộng hơn. So sánh với VLAN, VXLAN được mở rộng hơn về quy mô và khả năng triển khai chúng.
* Trong chuẩn định nghĩa cho VLAN 802.1q chỉ dành ra 12 bit để đánh VLAN-ID. VXLAN sử dụng 24 bit để đánh địa chỉ VLAN\_ID. Nghĩa là nó sẽ hỗ trợ không gian địa chỉ VXLAN\_ID lên tới 4 lần so với VLAN, tức là khoảng hơn 16 triệu. Điều này sẽ cung cấp đủ không gian để triển khai các quy mô mạng trong vài năm tới.
* VXLAN sử dụng IP (cả unicast và multicast) như phương tiện truyền. Sự phổ biến của mạng IP và các thiết bị cho phép đầu cuối sẽ cho phép khả năng mở rộng vượt trội tiến xa hơn rất nhiều so với VLAN sử dụng 802.1q hiện nay. Không gì có thể phủ nhận rằng các công nghệ khác có thể mở rộng được phạm vi của VLAN, nhưng không có gì có thể triển khai phổ biến như mạng IP.

17. MACVLAN và IPVLAN

Macvlan và IPvlan là những Linux Network Driver cho phép interface của host trực tiếp expose tới các VM hay các container chạy trên host đó.

##### **Linux Bridge**

Để hiểu hơn ta xét trường hợp sử dụng Linux Bridge (LB)trong môi trường ảo hóa network. LB hoạt động giống như một switch vậy lý bình thường. Khi triển khai LB, các VM hay các Container sẽ kết nối tới bridge và bridge sẽ kết nối với bên ngoài. Hình dưới tôi mô tả 2 VM kết nối tới bridge với eth0 cung cấp kết nối ra bên ngoài

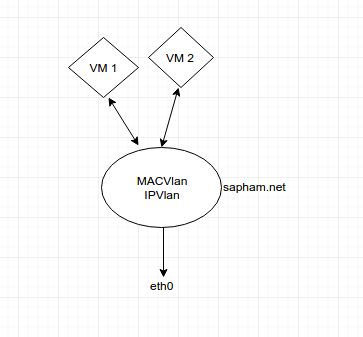


##### **Macvlan**

Macvlan cho phép một card interface vật lý có nhiều địa chỉ Mac và địa chỉ IP sử dụng macvlan sub-interface. Đó là sự khác nhau khi tạo sub-interface trên 1 interface vật lý sử dụng vlan. Với vlan sub-interface mỗi sub-interface thuộc về một vùng L2 khác nhau sử dụng vlan và tất cả sub-interface có cùng địa chỉ MAC. Với macvlan, mỗi sub-interface sẽ có địa chỉ MAC và IP khác nhau và có thể expose trực tiếp tới mạng bên ngoài. Interface của macvlan được sử dụng cho các ứng dụng ảo hóa, và mỗi mỗi interface vlan kết nối tới 1 container hay một VM. Mỗi container hay VM có thể lấy IP thông qua một DHCP Server bên ngoài.

MacVlan có 4 kiểu (Bridge, VEPA, Private, Passthrough). Bridge là kiểu hay được sử dụng nhất.

Hình dưới cả 2 VM sẽ trực tiếp expose với eth0 sử dụng macvlan sub-interface:



##### **IPVlan**

IPVlan tuơng tự với MacVlan nhưng khác nhau ở điểm các endpoint có cùng địa chỉ MAC. IPVlan hỗ trợ L2 và L3 mode.

Với IPVlan L2 Mode, Mỗi endpoint sử dụng chung địa chỉ MAC nhưng khác địa chỉ IP.

Với IPVlan L3 Mode, Các packet được route giữa các endpoint. Vì vậy ở mode này cho ta sự mở rộng tốt hơn.

18. TUN/TAP

Trong mạng máy tính, TUN/TAP là các thiết bị hạt nhân mạng ảo, đó là các thiết bị mạng được hỗ trợ hoàn toàn bằng phần mềm, chúng khác với các thiết bị mạng thông thường được sao lưu bằng phần cứng như các bộ điều hợp mạng (adapters). Điều này được yêu cầu để thiết lập một VPN trên gói VPS .

18. Macvtap

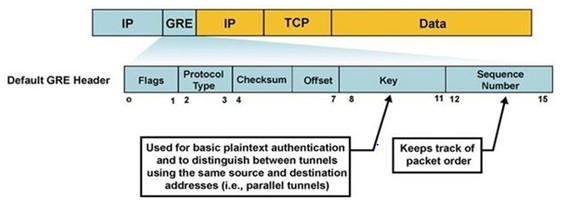
Macvtap là một trình điều khiển thiết bị mới có nghĩa là đơn giản hóa mạng cầu nối ảo hóa. Nó thay thế sự kết hợp của các trình điều khiển tun / tap và bridge với một mô-đun duy nhất dựa trên trình điều khiển thiết bị macvlan. Điểm cuối macvtap là thiết bị ký tự mà phần lớn tuân theo giao diện tun / tap ioctl và có thể được sử dụng trực tiếp bởi kvm / qemu và các trình siêu giám sát khác hỗ trợ giao diện tun / tap. Điểm cuối mở rộng giao diện mạng hiện có, thiết bị thấp hơn và có địa chỉ mac riêng trên cùng một phân đoạn ethernet. Thông thường, điều này được sử dụng để làm cho cả khách và máy chủ lưu trữ hiển thị trực tiếp trên công tắc mà máy chủ được kết nối.

19. GRE

GRE-Generic Routing Encapsulation là giao thức được phát triển đầu tiên bởi Cisco, Giao thức này sẽ đóng gói một số kiểu gói tin vào bên trong các IP tunnels để tạo thành các kết nối điểm-điểm (point-to-point) ảo. Các IP tunnel chạy trên hạ tầng mạng công cộng.

+ Tính năng:

GRE thêm vào tối thiểu 24 byte vào gói tin, trong đó bao gồm 20-byte IP header mới, 4 byte còn lại là GRE header. GRE có thể tùy chọn thêm vào 12 byte mở rộng để cung cấp tính năng tin cậy như: checksum, key chứng thực, sequence number.

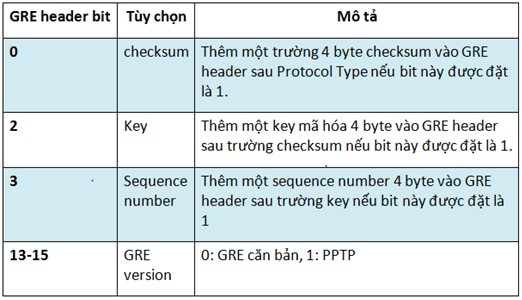


GRE là công cụ tạo tunnel khá đơn giản nhưng hiệu quả. Nó có thể tạo tunnel cho bấy kì giao thức lớp 3 nào. GRE cho phép những giao thức định tuyến hoạt động trên kênh truyền của mình. GRE không có cơ chế bảo mật tốt.

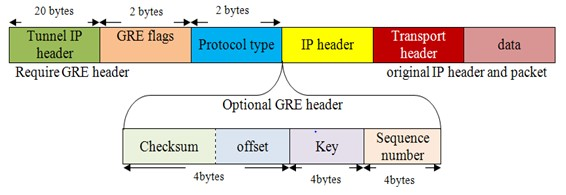
Trong khi đó, IPSec cung cấp sự tin cậy cao. Do đó nhà quản trị thường kết hợp GRE với IPSec để tăng tính bảo mật, đồng thời cũng hỗ trợ IPSec trong việc định tuyến và truyền những gói tin có địa chỉ IP Muliticast.

+ GRE header:

GRE header bản thân nó chứa đựng 4 byte, đây là kích cỡ nhỏ nhất của một GRE header khi không thêm vào các tùy chọn. 2 byte đầu tiên là các cờ (flags) để chỉ định những tùy chọn GRE. Những tùy chọn này nếu được active, nó thêm vào GRE header. Bảng sau mô tả những tùy chọn của GRE header.

****

Trong GRE header 2 byte còn lại chỉ định cho trường giao thức. 16 bits này xác định kiểu của gói tin được mang theo trong GRE tunnel. Hình sau mô tả cách mà một gói tin GRE với tất cả tùy chọn được gán vào một IP header và data.

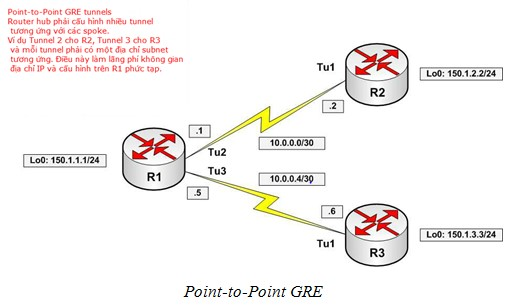


+ Phân loại GRE

RE là giao thức có thể đóng gói bất kì gói tin nào của lớp network. GRE cung cấp khả năng có thể định tuyến giữa những mạng riêng (private network) thông qua môi trường Internet bằng cách sử dụng các địa chỉ IP đã được định tuyến. GRE truyền thống là point-to-point, còn mGRE là sự mở rộng khái niệm này bằng việc cho phép một tunnel có thể đến được nhiều điểm đích, mGRE tunnel là thành phần cơ bản nhất trong DMVPN.

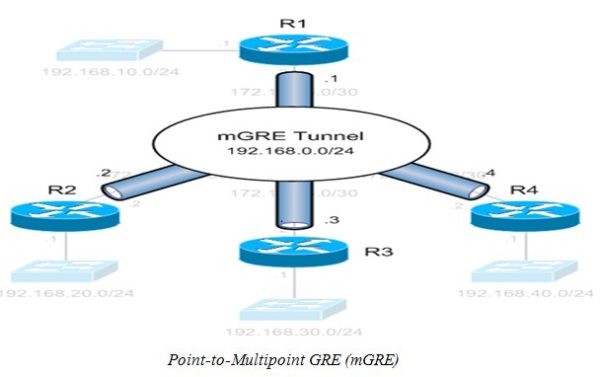
***Point-to-Point GRE***

Đối với các tunnel GRE point-to-point thì trên mỗi router spoke (R2 & R3) cấu hình một tunnel chỉ đến HUB (R1) ngược lại, trên router HUB cũng sẽ phải cấu hình hai tunnel, một đến R2 và một đến R3. Mỗi tunnel như vậy thì cần một địa chỉ IP. Giả sử mô hình trên được mở rộng thành nhiều spoke, thì trên R1 cần phải cấu hình phức tạp và tốn không gian địa chỉ IP.

****

***Point-to-Multipoint GRE (mGRE)***

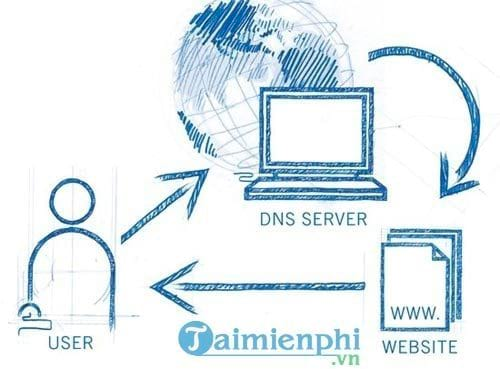
Như vậy, mGRE giải quyết được vấn đề đích đến là một địa chỉ multicast. Đây là tính năng chính của mGRE được dùng để thực thi Multicast VPN trong Cisco IOS. Tuy nhiên, trong mGRE, điểm cuối chưa được xác định nên nó cần một giao thức để ánh xạ địa chỉ tunnel sang địa chỉ cổng vật lý. Giao thức này được gọi là NHRP (Next Hop Resolution Protocol)



Đối với các mGRE Tunnel thì mỗi router chỉ có một Tunnel được cấu hình cùng một subnet logical.

20. DNS

**DNS** là một giao thức của mạng máy tính. Nhiệm vụ cơ bản của DNS là “biến” một tên miền thân thiện với người dùng, chẳng hạn như "**howstuffworks.com**" thành địa chỉ IP, ví dụ như 70.42.251.42 mà các máy tính sử dụng để nhận dạng lẫn nhau trên hệ thống mạng. Có thể ví DNS giống như GPS của máy tính trên mạng Internet.



Máy tính và các thiết bị kết nối mạng khác trên Internet sử dụng địa chỉ IP để “định tuyến” yêu cầu của người dùng tới trang web mà họ đang cố truy cập. Có thể hiểu nôm na, nó cũng giống như cách mà bạn quay số số điện thoại để kết nối với người mà bạn muốn gọi nói chuyện.

Nhờ cách sử dụng DNS nhanh nhất và hữu ích, người dùng không cần phải lưu một danh sách địa chỉ IP của riêng mình.Thay vào đó chỉ cần kết nối thông qua DNS nhanh nhất đó, Domain Name System hay Name Servers, quản lý một cơ sở dữ liệu khổng lồ map tên miền (domain name) tới địa chỉ IP.

21. DHCP

DHCP là từ viết tắt của Dynamic Host Configuration Protocol (Giao thức Cấu hình Host Động). Nó là giao thức cấp phát địa chỉ IP cho các thiết bị trên một mạng. Mọi thiết bị kết nối vào mạng đều cần một địa chỉ IP và địa chỉ IP đó thường được cấp phát bởi máy chủ DHCP (DHCP server) tích hợp trên router. Trên các hệ thống mạng lớn, một mình router không thể quản lý tất cả các thiết bị kết nối vào nó và do đó một máy chủ chuyên dụng sẽ chịu trách nhiệm cấp địa chỉ IP.

DHCP không chỉ cấp địa chỉ IP, nó còn cấp các thông số cần thiết cho hoạt động của mạng như subnet mask (mặt nạ mạng), default gateway (gateway mặc định), và dịch vụ DNS.

**Kiến trúc DHCP**

Có 3 thành phần bên trong kiến trúc DHCP bao gồm DHCP client, DHCP server, và DHCP relay agents.

**DHCP client** là thiết bị bất kỳ có thể kết nối vào mạng, và có thể giao tiếp với máy chủ DHCP. Nó có thể là điện thoại, máy tính nhưng cũng có thể là máy in mạng, máy chủ….

**DHCP server** là thiết bị cấp phát địa chỉ IP.

**DHCP relay agents** là thiết bị trung gian chuyển tiếp yêu cầu giữa DHCP client và DHCP server. Chúng không phải là thành phần thiết yếu của một mạng thông thường. Tuy nhiên, khi làm việc với các hệ thống mạng lớn, phức tạp, chúng lại trở nên rất cần thiết.

**DHCP Lease**

Một địa chỉ IP, khi được cấp phát cho một thiết bị, sẽ có vòng đời nhất định, thường là 24 giờ. Điều này có nghĩa, nếu bạn kết nối máy tính vào một mạng, nó sẽ được cấp một địa chỉ IP và bạn có thể sử dụng IP đó trong vòng 24 giờ.

Trong khoảng thời gian 24 giờ, nếu bạn ngắt kết nối khỏi mạng và sau đó kết nối lại, bạn vẫn sẽ sử dụng địa chỉ IP đã được cấp trước đó. Tuy nhiên, khi hết 24 giờ, máy tính của bạn sẽ được cấp một địa chỉ IP mới.

Ngoài ra, nếu bạn gặp vấn đề với IP hiện có, bạn có thể yêu cầu cấp mới địa chỉ IP, không cần đợi IP hiện tại hết vòng đời.

Bạn có thể tìm thấy các thiết lập này trong phần cài đặt mạng trên máy tính, hoặc trong các thiết lập WiFi trên điện thoại.

**Ý nghĩa của DHCP**

DHCP là yếu tố cần thiết quyết định số lượng thiết bị có thể kết nối vào một mạng. Nó đảm bảo tất cả các thiết bị trên mạng đều có địa chỉ IP và không có thiết bị nào bị trùng IP. Không có DHCP, các thiết bị trên mạng có thể gặp lỗi xung đột IP khiến cho việc quản trị mạng trở nên khó khăn. Gán địa chỉ IP theo cách thủ công, xử lý lỗi xung đột IP là những công việc tẻ nhạt, tốn thời gian ngay cả trên những hệ thống mạng nhỏ. Đối với các hệ thống mạng lớn hơn, đó gần như là điều bất khả thi.

22. TCP và UDP

TCP và UDP đều là các giao thức được sử dụng để gửi các bit dữ liệu - được gọi là các gói tin - qua Internet. Cả hai giao thức đều được xây dựng trên giao thức IP. Nói cách khác, dù bạn gửi gói tin qua TCP hay UDP, gói này sẽ được gửi đến một địa chỉ IP. Những gói tin này được xử lý tương tự bởi vì chúng được chuyển tiếp từ máy tính của bạn đến router trung gian và đến điểm đích

TCP và UDP không phải là giao thức duy nhất hoạt động trên IP, tuy nhiên, chúng được sử dụng rộng rãi nhất.

## **Cách thức hoạt động của TCP**

TCP là giao thức được sử dụng phổ biến nhất trên Internet. Khi bạn yêu cầu một trang web trong trình duyệt, máy tính sẽ gửi các gói tin TCP đến địa chỉ của máy chủ web, yêu cầu nó gửi lại trang web. Máy chủ web phản hồi bằng cách gửi một luồng các gói tin TCP, mà trình duyệt web của bạn kết hợp với nhau để tạo thành trang web. Khi click vào liên kết, đăng nhập, đăng nhận xét hoặc làm bất kỳ điều gì khác, trình duyệt web của bạn sẽ gửi gói tin TCP tới máy chủ và máy chủ gửi lại các gói tin cho TCP.

Giao thức TCP có độ tin cậy cao, các gói tin được gửi bằng TCP sẽ được theo dõi do vậy dữ liệu sẽ không bị mất hoặc hỏng trong quá trình vận chuyển. Đó là lý do tại sao file tải xuống không bị hỏng ngay cả khi mạng có vấn đề. Tất nhiên, nếu bên nhận hoàn toàn ngoại tuyến, máy tính của bạn sẽ từ bỏ và bạn sẽ thấy một thông báo lỗi ghi nó không thể giao tiếp với máy chủ lưu trữ từ xa.

Giao thức TCP đạt được điều này theo hai cách. Đầu tiên, nó yêu cầu các gói tin bằng cách đánh số chúng. Thứ hai, nó kiểm tra lỗi bằng cách yêu cầu bên nhận gửi phản hồi đã nhận được cho bên gửi. Nếu bên gửi không nhận được phản hồi đúng, nó có thể gửi lại gói tin để đảm bảo bên nhận nhận chúng một cách chính xác

## **Cách thức hoạt động của UDP**

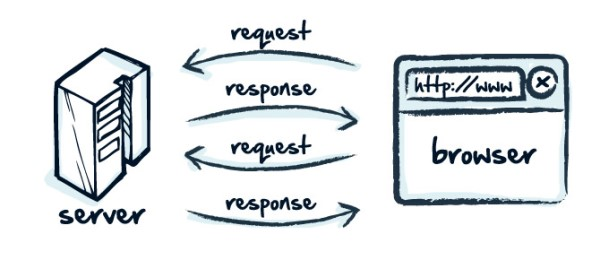
Giao thức UDP hoạt động tương tự như TCP, nhưng nó bỏ qua quá trình kiểm tra lỗi. Khi một ứng dụng sử dụng giao thức UDP, các gói tin được gửi cho bên nhận và bên gửi không phải chờ để đảm bảo bên nhận đã nhận được gói tin, do đó nó lại tiếp tục gửi gói tin tiếp theo. Nếu bên nhận bỏ lỡ một vài gói tin UDP, họ sẽ mất vì bên gửi không gửi lại chúng. Do đó thiết bị có thể giao tiếp nhanh hơn.

UDP được sử dụng khi tốc độ nhanh và không cần thiết sửa lỗi. Ví dụ, UDP thường được sử dụng cho các chương trình phát sóng trực tiếp và game online.

Giả dụ, bạn đang xem phát video trực tiếp, thường được phát bằng UDP thay vì TCP. Máy chủ sẽ gửi một luồng liên tục các gói tin UDP tới máy tính đang xem. Nếu bạn mất kết nối trong vài giây, video sẽ bị dừng hoặc bị giật trong giây lát và sau đó chuyển sang bit hiện tại của chương trình phát sóng. Nếu bạn chỉ bị mất gói tin nhỏ, video hoặc âm thanh có thể bị méo trong giây lát vì video sẽ tiếp tục phát mà không có dữ liệu bị thiếu.

Điều này hoạt động tương tự trong các trò chơi trực tuyến. Nếu bạn bỏ lỡ một số gói tin UDP, nhân vật người chơi có thể dịch chuyển trên bản đồ khi bạn nhận gói tin UDP mới. Việc bỏ qua sửa lỗi của TCP sẽ giúp tăng tốc kết nối trò chơi và giảm độ trễ.

23. HTTP

HTTP là chữ viết tắt của HyperText Transfer Protocol (giao thức truyền tải siêu văn bản). Đây là một giao thức ứng dụng trong bộ các giao thức TCP/IP (gồm một nhóm các giao thức nền tảng cho internet).

HTTP hoạt động dựa trên mô hình Client – Server. Trong mô hình này, các máy tính của người dùng sẽ đóng vai trò làm máy khách (Client). Sau một thao tác nào đó của người dùng, các máy khách sẽ gửi yêu cầu đến máy chủ (Server) và chờ đợi câu trả lời từ những máy chủ này. Để có thể nói chuyện được với nhau, các máy chủ và máy khách phải thực hiện việc trao đổi thông qua các giao thức. Một trong những giao thức được sử dụng thường xuyên nhất chính là HTTP.

Khi gõ một địa chỉ Web URL vào trình duyệt Web, một lệnh HTTP sẽ được gửi tới Web server để ra lệnh và hướng dẫn nó tìm đúng trang Web được yêu cầu. Trang Web này sau đó sẽ được kéo về và mở trên trình duyệt Web. Nói đơn giản hơn, HTTP là giao thức giúp cho việc truyền tải file từ một Web server vào một trình duyệt Web để người dùng có thể xem một trang Web đang hiện diện trên trình duyệt.

**Khi dùng trình duyệt truy cập Web, thường gặp các thông báo lỗi khác nhau như sau:**

-Lỗi 404 hay Http 404 tức là lỗi không tồn tại địa chỉ bạn đang truy cập

-Lỗi 401: lỗi này là truy cập vào nơi yêu cầu xác thực, nhưng không vượt qua được sẽ có lỗi này.

-Lỗi 500: lỗi này thường do Web server mà bạn truy cập bị lỗi nên không thể truy cập vào được.

Ngoài ra Http 200 tức là truy cập thành công.